Title (en)

MUTUAL DIVISION CIRCUIT

Publication

EP 0431629 A3 19930721 (EN)

Application

EP 90123470 A 19901206

Priority

- JP 31940489 A 19891208
- JP 32111889 A 19891211
- JP 33588389 A 19891225
- JP 33588489 A 19891225

Abstract (en)

[origin: EP0431629A2] A mutual division circuit includes a single mutual division unit or a plurality of cascaded mutual division units for dividing a polynomial including a first input polynomial Ri-1(X) as a factor by a second input polynomial Qi-1(X), thereby to determine a quotient and a remainder Ri(X), determining an overall quotient lambda i(X) from the quotient and a third input polynomial lambda i-1(X), and producing the remainder Ri(X), the first input polynomial Ri-1(X) or the second input polynomial Qi-1(X), and the overall quotient lambda i(X) as a first output polynomial Ri(X), a second output polynomial Qi(X), and a third output polynomial lambda i(X), respectively. The mutual division circuit also has a data selector (42) for receiving, at an input port thereof, respective initial polynomials of the first, second, and third input polynomials, and supplying output data to the single mutual division unit or a first one of the cascaded mutual division units, and a feedback or data bus (45) for supplying output data from the single mutual division unit or a last one of the the cascaded mutual division units to another input port of the data selector (42). The single mutual division unit or the cascaded mutual division units are used a plurality of times for carrying out arithmetic operations therein. <IMAGE>

IPC 1-7

G06F 7/72

IPC 8 full level

G06F 7/72 (2006.01); **H03M 13/03** (2006.01)

CPC (source: EP KR US)

G06F 7/726 (2013.01 - EP US); **H03M 7/00** (2013.01 - KR); **H03M 13/033** (2013.01 - EP US)

Citation (search report)

- [YD] EP 0152702 A2 19850828 - SONY CORP [JP]
- [Y] EP 0271082 A2 19880615 - MATSUSHITA ELECTRIC IND CO LTD [JP]
- MENDELBAUM D. M.: "ON ITERATIVE ARRAYS FOR THE EUCLIDEAN ALGORITHM OVER FINITE FIELDS.", IEEE TRANSACTIONS ON COMPUTERS., IEEE SERVICE CENTER, LOS ALAMITOS, CA., US, vol. 38., no. 10., 1 October 1989 (1989-10-01), US, pages 1473 - 1478., XP000070487, ISSN: 0018-9340, DOI: 10.1109/12.35844
- IEEE TRANSACTIONS ON COMPUTERS, vol. 38, no. 10, October 1989, pages 1473-1478, New York, US; D.M. MANDELBAUM: "On iterative arrays for the Euclidean algorithm over finite fields"

Cited by

EP0567269A3; NL1003335C2; EP0786868A1; US5736893A; US5909144A

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

EP 0431629 A2 19910612; **EP 0431629 A3 19930721**; KR 910013754 A 19910808; US 5185711 A 19930209

DOCDB simple family (application)

EP 90123470 A 19901206; KR 900020087 A 19901207; US 62323590 A 19901206